UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/760,262	01/12/2001	Gabor Wieser	P-A790	2574

7590 06/25/2004

W. Thomas Timmons
The White House on Turtle Creek
2401 Turtle Creek Boulevard
Dallas, TX 75219-4760

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/760,262	WIESER, GABOR
	Examiner	Art Unit
	Ellen C Tran	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 12 January 2001, with acknowledgement of continuing date 13 January 2000.

2. Claims 1-12 are currently pending in this application. Claims 1, 10, 11, and 12 are independent claims.

Claim Rejections - 35 USC § 112

3. Claim 6 is rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The claim(s) are narrative in form and replete with indefinite and functional or operational language. The claim(s) must be in one sentence form only. Note the format of the claims in the patent(s) cited. Claim 6 contains three sentences. (MPEP 7.34.15)

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. **Claims 1-12** are rejected under 35 U.S.C. 102(e) as being anticipated by Luyster U.S. Patent No. 6,182,216 (hereinafter '216).

As to independent claim 1, "A method for encrypting binary data comprising of blocks of tokens, which in turn are comprised of bits" and "making multiple copies of it, and moving the significant digits into the lower bits of the tokens according to a predefined pattern; modifying the said significant digits by adding their location to their values; replacing the other (non-significant) binary digits by pseudo-random bits; rotating segments, which are groups of tokens, of the resulting block by values derived from the count of the bits with a predetermined value of one or zero in the said segments; modifying the tokens by adding their locations to their values; rotating the resulting block by a value derived from the count of the bits" is taught in '216 col. 15, line 60 through col. 16, line 12;

"into a binary cipher, comprising the steps of: segregating a block of binary data from the input stream" is shown in '216 col. 18, line 54-68;

"with a predetermined value of one or zero in the block; performing a token by token substitution transformation on the block by using a private key, which is a permutation of all possible tokens; performing a token by token transposition transformation on the block, using a private key, which is the permutation of all possible locations" is disclosed in '216 col. 15, lines 40-59.

As to dependent claim 2 "wherein the segregation of the blocks is done under the control of two parameters, the t token length (number of bits in a token) and the b block length (number of tokens in a block)" is taught in '216 col. 22, lines 31-41.

As to dependent claim 3, "further comprising the step of inserting one or more authentication tokens into the data at any desired location" is shown in '216 col. 22, lines 13-21.

As to dependent claim 4, "further comprising the step of making a plurality of copies of the data according to parameter c (the number of copies), and thus generating a complete block" is disclosed in '216 col. 23, lines 39-46.

As to dependent claim 5, "further comprising a method to change the frequency distribution of the tokens in the said complete block by the following steps: moving the significant bits of each token to the lowest bits according to a pattern for each copy of the data; summing the location as a binary number and value as a binary number modulo 2' for each token and changing the value of the token to this result; filling the non-significant bits of the tokens with pseudo-random bits; generating an S_i rotation amount for each segment and rotating it; summing the location as a binary number and value as a binary number modulo 2' for each token again; generating an S_i rotation amount for the complete block and rotating it" is taught in '216 col. 22, lines 42-65.

As to dependent claim 6, "wherein the pattern for moving the significant bits is a further parameter of the system. This pattern defines which bits are significant in each copy. All combinations work, which satisfy the following criteria: every block has to have at least two significant bits and each source bit has to be represented at least in one copy as significant" is shown in '216 col. 22, lines 42-65.

As to dependent claim 7, "further comprising a method to generate a count for segment rotation S_i by the following steps: XORing the bits of the bit displacement value into the token displacement value in reverse order; rotating the count by one bit to the left; replacing the lowest order bit by the complement of the second lowest order bit" is disclosed in '216 col. 24, line 38 through col. 25, line 59.

As to dependent claim 8, "further comprising a method to generate a count for complete block rotation S_i by the following steps: XORing the bits of the bit displacement value into the token displacement and segment displacement values in reverse order; rotating the count by one bit to the left" is taught in '216 col. 36, lines 61-68.

As to dependent claim 9, "further comprising a method to encrypt the data by the following steps in any sequence: performing a token by token substitution transformation on the modified block by using a private key, which is a permutation of all possible tokens; performing a token by token transposition transformation on the block resulting from the substitution, using a private key, which is the permutation of all possible locations" is shown in '216 col. 22, lines 6-65.

As to independent claim 10, "The method to mask token frequencies comprising the steps of: distributing the bits of a token among a plurality of tokens; moving these bits to the lowest order bits of the tokens; replacing the other bits with pseudo-random bits" is disclosed in '216 col. 22, lines 6-25;

"summing the location as a binary number and value as a binary number modulo 2' for each token" is taught in '216 col. 24, lines 62-65.

As to independent claim 11, "The method to use the count of bits with a predetermined value of one or zero in a bit string as the rotational value for the string" is shown in '216 col. 21, lines 5-38.

As to independent claim 12, "A method for decrypting binary data from a binary cipher, comprising the steps of: performing a token by token transposition transformation on the block, using a private key, which is the reversal key of the encryption key; performing a token by token substitution transformation on the block by using a private key, which is the reversal key of the encryption key; rotating the resulting block by a value derived from the count of the bits with a value of one in the block; modifying the tokens by subtracting their locations from their values; rotating segments of the resulting block by values derived from the count of the bits with a value of one in the said segments; modifying the tokens by subtracting their locations from their values; merging the bits from all the copies according to the reversal pattern of the encryption pattern" is disclosed in '216 col. 25, line 65 through col. 26, line 11.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Ellen Tran,
Patent Examiner
Technology Center 2134
14 June 2004